UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/523,840	08/18/2005	Olivier Billet	032326-293	4245

21839 7590 04/22/2009

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
SMITHERS, MATTHEW	

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
04/22/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

Office Action Summary	Application No.	Applicant(s)	
	10/523,840	BILLET ET AL.	
	Examiner	Art Unit	
	Matthew B. Smithers	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 February 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 February 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/18/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

The information disclosure statement filed February 18, 2005 has been placed in the application file and the information referred to therein has been considered as to the merits.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-14 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1-11 provides for the use of calculating points on an elliptic curve, but, since the claim does not set forth any steps involved in the method/process, it is unclear what method/process applicant is intending to encompass. A claim is indefinite where it merely recites a use without any active, positive steps delimiting how this use is actually practiced.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-11 are rejected under 35 U.S.C. 101 because the claimed recitation of a use, without setting forth any steps involved in the process, results in an improper definition of a process, i.e., results in a claim which is not a proper process claim under 35 U.S.C. 101. See for example *Ex parte Dunki*, 153 USPQ 678 (Bd.App. 1967) and *Clinical Products, Ltd.* v. *Brenner*, 255 F. Supp. 131, 149 USPQ 475 (D.D.C. 1966).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-11 are rejected under 35 U.S.C. 102(e) as being anticipated by US 6,778,666 granted to Kuzmich et al.

Regarding claim 1, Kuzmich meets the claimed limitations as follows:

“A method of universal calculation on points on an elliptic curve, wherein the elliptic curve is defined by a quartic equation and identical programmed calculation means are used to carry out an operation of addition of points, an operation of doubling of points, and an operation of addition of a neutral point, the calculation means comprising a

central processing unit associated with a memory." see Abstract; column 6, line 62 to column 14, line 14.

Regarding claim 2, Kuzmich meets the claimed limitations as follows:

"A method according to claim 1, wherein the elliptic curve is defined by a quartic equation of the type: V.sup.2=b.U.sup.4+a.U.sup.3W+UW.sup.3, (U:V:W) being Jacobi projective coordinates of a point P on the elliptic curve, and a, b being parameters of the elliptic curve, a point with coordinates (0:0:1) being a neutral point O of the elliptic curve, a point with coordinates (U:-V:W) being an inverse point of the point P with coordinates (U:V:W) ." see Abstract; column 6, line 62 to column 14, line 14.

Regarding claim 3, Kuzmich meets the claimed limitations as follows:

"A method according to claim 2, in which the point P is also defined in affine coordinates (X, Y), the affine coordinates (X, Y) and the Jacobi projective coordinates (U:V:W) of the point P being linked by the relationships: (X, Y)=(U/W, V/W.sup.2) ." see Abstract; column 6, line 62 to column 14, line 14.

Regarding claim 4, Kuzmich meets the claimed limitations as follows:

"A method according to claim 2, in which, in order to carry out the addition of a first point P1 defined by first Jacobi projective coordinates (U1:V1:W1) and a second point P2 defined by second Jacobi projective coordinates (U2:V2:W2), the coordinates of the first point P1 and those of the second point P2 being stored in first and second registers in the memory, the first point and the second point belonging to the elliptic curve, the programmed calculation means calculate third Jacobi projective coordinates (U3:V3:W3) defining a third point P3, the result of the addition, by the following

equations: U3 = .times. 2. .times. b . U1 2 . U2 2 + (aU1 . U2 + W1 . W2) . (U1 . W2 + W1 . U2) + .times. 2 .times. V1 . V2 V3 = .times. (U1 2 . V2 + U2 2 . V1) * .times. (4 .times. b . (U1 . W2 + U2 . W1) . W1 . W2 - .times. 8 .times. b 2 . (U1 . U2) 2 + .times. a . [(2 .times. W1 . W2) 2 - (aU1 . U2 + W1 . W2) 2] + .times. (W1 2 . V2 + W2 2 . V1) * .times. [(aU1 . U2 + W1 . W2) 2 - (2 .times. aU1 . U2) 2 + .times. 4 .times. bU1 . U2 . (W1 . U2 + U1 . W2)] - .times. 4 .times. bU1 . U2 . (U1 . W1 . V2 + U2 . W2 . V1) .times. (aU1 . U2 - W1 . W2) W3 = (aU1 . U2 - W1 . W2) 2 - 4 .times. bU1 . U2 .times. .times. (U1 . W2 + U2 . W1) and then store the third projective coordinates (U3:V3:W3) in third registers in the memory." see Abstract; column 6, line 62 to column 14, line 14.

Regarding claim 5, Kuzmich meets the claimed limitations as follows:

"A method according to claim 1, in which the elliptic curve is a curve comprising a single point of order two and is defined by a quartic equation of the type: V.sup.2=.epsilon..U.sup.4-2.delta.. U.sup.2.W.sup.2+W.sup.4, (U:V:W) being Jacobi projective coordinates of a point P on the elliptic curve, and .epsilon., .delta. being parameters of the elliptic curve, the point with coordinates (0:1:1) being the neutral point O of the elliptic curve, the point with coordinates (-U:+V:W) being the inverse point (-P) of the point P (U:V:W) ." see Abstract; column 6, line 62 to column 14, line 14.

Regarding claim 6, Kuzmich meets the claimed limitations as follows:

"A method according to claim 5, in which, in order to carry out the addition of the first point P1 defined by first Jacobi projective coordinates (U1:V1:W1) and the second point P2 defined by second Jacobi projective coordinates (U2:V2:W2),the coordinates of the

first point P1 and those of the second point P2 being stored in first and second registers in the memory, the first point and the second point belonging to the elliptic curve, the programmed calculation means calculate third Jacobi projective coordinates (U3:V3:W3) defining a third point P3, the result of the addition, by the following equations: U3=U1.W1.V2+V1.U2.W2 V3=[(W1.W2).sup.2+.epsilon.(U1.U2).sup.2]*[V1.V2-2.delta.U1.U2.W1.W2]+2.d-elta..U1.U2.W1.W2(U1.sup.2W2.sup.2+W1.sup.2U2.sup.2) W3=(W1.W2).sup.2-.epsilon.(U1.U2).sup.2 and then store the third projective coordinates (U3:V3:W3) in the third registers in the memory." see Abstract; column 6, line 62 to column 14, line 14.

Regarding claim 7, Kuzmich meets the claimed limitations as follows: "A method according to claim 5, in which the elliptic curve is defined in affine coordinates by an equation of the type: Y.sup.2=.epsilon..X.sup.4-2.delta..X.sup.2+1 (X, Y) being affine coordinates of a point P on the elliptic curve." see Abstract; column 6, line 62 to column 14, line 14.

Regarding claim 8, Kuzmich meets the claimed limitations as follows: "A method according to claim 7, in which, in order to carry out the addition of the first point P1 defined by first affine coordinates (X1, Y1) and the second point P2 defined by second affine coordinates (X2, Y2), the coordinates of the first point P1 and those of the second point P2 being stored in first and second registers in the memory, the first point P1 and the second point P2 belonging to the elliptic curve, the programmed calculation means calculate third affine coordinates (X3, Y3) defining a third point P3, the result of the addition, by the following equations: X3=(X1.Y2+Y1.X2)/[1-

.epsilon.(X1.X2).sup.2]Y3={[1+.epsilon.(X1.X2).sup.2]- .[Y1.Y2-
2.delta..X1.X2]+2.delta..X1.X2.(X1.sup.2+X2.sup.2)}/[1-.epsilon.(X- 1.X2).sup.2]and then store the third affine coordinates (X3, Y3) in the third registers in the memory." see Abstract; column 6, line 62 to column 14, line 14.

Regarding claim 9, Kuzmich meets the claimed limitations as follows: "A method according to claim 5, in which the elliptic curve is a curve comprising three points of order two and has .epsilon.=1 as a parameter." see Abstract; column 6, line 62 to column 14, line 14.

Regarding claim 10, Kuzmich meets the claimed limitations as follows: "Use of a calculation method according to claim 1 in a scalar multiplication calculation method applied to points on an elliptic curve." see Abstract; column 6, line 62 to column 14, line 14.

Regarding claim 1, Kuzmich meets the claimed limitations as follows: "Use of a calculation method according to claim 1 in a cryptographic method." see Abstract; column 6, line 62 to column 14, line 14.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-14 are rejected under 35 U.S.C. 102(e) as being anticipated by Liardet et al disclosed in "Preventing SPA/DPA in ECC Systems Using Jacobi Form".

Regarding claim 1, Liardet meets the claimed limitations as follows:

"A method of universal calculation on points on an elliptic curve, wherein the elliptic curve is defined by a quartic equation and identical programmed calculation means are used to carry out an operation of addition of points, an operation of doubling of points, and an operation of addition of a neutral point, the calculation means comprising a central processing unit associated with a memory." see Abstract; Introduction, pages 394-399.

Regarding claim 2, Liardet meets the claimed limitations as follows:

"A method according to claim 1, wherein the elliptic curve is defined by a quartic equation of the type: V.sup.2=b.U.sup.4+a.U.sup.3W+UW.sup.3, (U:V:W) being Jacobi projective coordinates of a point P on the elliptic curve, and a, b being parameters of the elliptic curve, a point with coordinates (0:0:1) being a neutral point O of the elliptic curve, a point with coordinates (U:-V:W) being an inverse point of the point P with coordinates (U:V:W) ." see Abstract; Introduction, pages 394-399.

Regarding claim 3, Liardet meets the claimed limitations as follows:

"A method according to claim 2, in which the point P is also defined in affine coordinates (X, Y), the affine coordinates (X, Y) and the Jacobi projective coordinates (U:V:W) of the point P being linked by the relationships: (X, Y)=(U/W, V/W.sup.2) ." see Abstract; Introduction, pages 394-399.

Regarding claim 4, Liardet meets the claimed limitations as follows:

"A method according to claim 2, in which, in order to carry out the addition of a first point P1 defined by first Jacobi projective coordinates (U1:V1:W1) and a second point P2 defined by second Jacobi projective coordinates (U2:V2:W2), the coordinates of the first point P1 and those of the second point P2 being stored in first and second registers in the memory, the first point and the second point belonging to the elliptic curve, the programmed calculation means calculate third Jacobi projective coordinates (U3:V3:W3) defining a third point P3, the result of the addition, by the following equations: U3 = .times. 2. .times. b . U1 2 . U2 2 + (aU1 . U2 + W1 . W2) . (U1 . W2 + W1 . U2) + .times. 2 .times. V1 . V2 V3 = .times. (U1 2 . V2 + U2 2 . V1) * .times. (4 .times. b . (U1 . W2 + U2 . W1) . W1 . W2 - .times. 8 .times. b 2 . (U1 . U2) 2 + .times. a . [(2 .times. W1 . W2) 2 - (aU1 . U2 + W1 . W2) 2] + .times. (W1 2 . V2 + W2 2 . V1) * .times. [(aU1 . U2 + W1 . W2) 2 - (2 .times. aU1 . U2) 2 + .times. 4 .times. bU1 . U2 . (W1 . U2 + U1 . W2)] - .times. 4 .times. bU1 . U2 . (U1 . W1 . V2 + U2 . W2 . V1) .times. (aU1 . U2 - W1 . W2) W3 = (aU1 . U2 - W1 . W2) 2 - 4 .times. bU1 . U2 .times. .times. (U1 . W2 + U2 . W1) and then store the third projective coordinates (U3:V3:W3) in third registers in the memory." see Abstract; Introduction, pages 394-399.

Regarding claim 5, Liardet meets the claimed limitations as follows:

"A method according to claim 1, in which the elliptic curve is a curve comprising a single point of order two and is defined by a quartic equation of the type: V.sup.2=.epsilon..U.sup.4-2.delta.. U.sup.2.W.sup.2+W.sup.4, (U:V:W) being Jacobi projective coordinates of a point P on the elliptic curve, and .epsilon., .delta. being

parameters of the elliptic curve, the point with coordinates (0:1:1) being the neutral point O of the elliptic curve, the point with coordinates (-U:+V:W) being the inverse point (-P) of the point P (U:V:W) ." see Abstract; Introduction, pages 394-399.

Regarding claim 6, Liardet meets the claimed limitations as follows:

"A method according to claim 5, in which, in order to carry out the addition of the first point P1 defined by first Jacobi projective coordinates (U1:V1:W1) and the second point P2 defined by second Jacobi projective coordinates (U2:V2:W2),the coordinates of the first point P1 and those of the second point P2 being stored in first and second registers in the memory, the first point and the second point belonging to the elliptic curve, the programmed calculation means calculate third Jacobi projective coordinates (U3:V3:W3) defining a third point P3, the result of the addition, by the following equations: U3=U1.W1.V2+V1.U2.W2

V3=[(W1.W2).sup.2+.epsilon.(U1.U2).sup.2]*[V1.V2-2.delta.U1.U2.W1.W2]+2.d-elta..U1.U2.W1.W2(U1.sup.2W2.sup.2+W1.sup.2U2.sup.2) W3=(W1.W2).sup.2-.epsilon.(U1.U2).sup.2 and then store the third projective coordinates (U3:V3:W3) in the third registers in the memory." see Abstract; Introduction, pages 394-399.

Regarding claim 7, Liardet meets the claimed limitations as follows:

"A method according to claim 5, in which the elliptic curve is defined in affine coordinates by an equation of the type: Y.sup.2=.epsilon..X.sup.4-2.delta..X.sup.2+1 (X, Y) being affine coordinates of a point P on the elliptic curve." see Abstract; Introduction, pages 394-399.

Regarding claim 8, Liardet meets the claimed limitations as follows:

"A method according to claim 7, in which, in order to carry out the addition of the first point P1 defined by first affine coordinates (X1, Y1) and the second point P2 defined by second affine coordinates (X2, Y2), the coordinates of the first point P1 and those of the second point P2 being stored in first and second registers in the memory, the first point P1 and the second point P2 belonging to the elliptic curve, the programmed calculation means calculate third affine coordinates (X3, Y3) defining a third point P3, the result of the addition, by the following equations: X3=(X1.Y2+Y1.X2)/[1-.epsilon.(X1.X2).sup.2]Y3={[1+.epsilon.(X1.X2).sup.2]- .[Y1.Y2-2.delta..X1.X2]+2.delta..X1.X2.(X1.sup.2+X2.sup.2)}/[1-.epsilon.(X- 1.X2).sup.2]and then store the third affine coordinates (X3, Y3) in the third registers in the memory." see Abstract; Introduction, pages 394-399.

Regarding claim 9, Liardet meets the claimed limitations as follows:

"A method according to claim 5, in which the elliptic curve is a curve comprising three points of order two and has .epsilon.=1 as a parameter." see Abstract; Introduction, pages 394-399.

Regarding claim 10, Liardet meets the claimed limitations as follows:

"Use of a calculation method according to claim 1 in a scalar multiplication calculation method applied to points on an elliptic curve." see Abstract; Introduction, pages 394-399.

Regarding claim 11, Liardet meets the claimed limitations as follows:

"Use of a calculation method according to claim 1 in a cryptographic method." see Abstract; Introduction, pages 394-399.

Regarding claim 12, Liardet meets the claimed limitations as follows: "An electronic component comprising programmed calculation means for implementing a method according to claim 1, the calculation means comprising in particular a central processing unit associated with a memory." see Abstract; Introduction, pages 394-399.

Regarding claim 13, Liardet meets the claimed limitations as follows: "An electronic component comprising means for implementing a cryptographic algorithm using a method according to claim 1." see Abstract; Introduction, pages 394-399.

Regarding claim 14, Liardet meets the claimed limitations as follows: "A smart card comprising an electronic component according to claim 12." see Abstract; Introduction, pages 394-399.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Hisil et al., "Faster Group Operations on Elliptic Curves".

B. Macleod, "14-term Arithmetic Progressions on Quartic Elliptic Curves".

C. Hisil et al., "New Formulae for Efficient Elliptic Curve Arithmetic".

D. Girard, "The Group Of Weierstrass Points Of A Plane Quartic With At Least Eight Hyperflexes".

E. Joye (US 20040247114).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B. Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew B Smithers/
Primary Examiner, Art Unit 2437